Computer Network Security Literature Review Papers

Right here, we have countless books **Computer Network Security Literature Review Papers** and collections to check out. We additionally present variant types and also type of the books to browse. The agreeable book, fiction, history, novel, scientific research, as capably as various supplementary sorts of books are readily nearby here.

As this Computer Network Security Literature Review Papers, it ends occurring bodily one of the favored ebook Computer Network Security Literature Review Papers collections that we have. This is why you remain in the best website to look the incredible book to have.

Handbook of Computer Networks and Cyber Security Springer Nature
This book features selected research papers presented at the Second International Conference on Computing, Communications, and Cyber-Security (IC4S 2020), organized in Krishna Engineering College (KEC), Ghaziabad, India, along with Academic Associates; Southern Federal University, Russia; IAC Educational, India; and ITS Mohan Nagar, Ghaziabad, India during 3–4 October 2020. It includes innovative work from researchers, leading innovators, and professionals in the area of communication and network technologies, advanced computing technologies, data analytics and intelligent learning, the latest electrical and electronics trends, and security and privacy issues.

Cryptography: Breakthroughs in Research and Practice IGI Global
This two-volume set (CCIS 955 and CCIS 956) constitutes the refereed proceedings of the Second International Conference on Advanced Informatics for Computing Research, ICAICR 2018, held in Shimla, India, in July 2018. The 122 revised full papers presented were carefully reviewed and selected from 427 submissions. The papers are organized in topical sections on computing methodologies; hardware; information systems; networks; security and privacy; computing methodologies.

Methods, Implementation, and Application of Cyber Security Intelligence and Analytics National Academies Press
This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book's website at Springer.com.

ICT and Data Sciences CRC Press
As we enter the Industrial Revolution 4.0, demands for an increasing degree of trust and privacy protection continue to be voiced. The development of blockchain technology is very important because it can help frictionless and transparent financial transactions and improve the business experience, which in turn has far-reaching effects for economic, psychological, educational and organizational improvements in the way we work, teach, learn and care for ourselves and each other. Blockchain is an eccentric technology, but at the same time, the least understood and most disruptive technology of the day. This book covers the latest technologies of cryptocurrencies and blockchain technology and their applications. This book discusses the blockchain and cryptocurrencies related issues and also explains how to provide the security differently through an algorithm, framework, approaches, techniques and mechanisms. A comprehensive understanding of what blockchain is and how it works, as well as insights into how it will affect the future of your organization and industry as a whole and how to integrate blockchain technology into your business strategy. In addition, the book explores the blockchain and its with other technologies like Internet of Things, big data and artificial intelligence, etc.

Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020) **Springer Nature**
This book provides stepwise discussion, exhaustive literature review, detailed analysis and discussion, rigorous experimentation results (using several analytics tools), and an application-oriented approach that can be demonstrated with respect to data analytics using artificial intelligence to make systems stronger (i.e., impossible to breach). We can see many serious cyber breaches on Government databases or public profiles at online social networking in the recent decade. Today artificial intelligence or machine learning is redefining every aspect of cyber security. From improving organizations' ability to anticipate and thwart breaches, protecting the proliferating number of threat surfaces with Zero Trust Security frameworks to making passwords obsolete, AI and machine learning are essential to securing the perimeters of any business. The book is useful for researchers, academics, industry players, data engineers, data scientists, governmental organizations, and non-governmental organizations.

Pervasive Information Security and Privacy Developments: Trends and Advancements **Springer Science & Business Media**
The seven volumes LNCS 12249-12255 constitute the refereed proceedings of the 20th International Conference on Computational Science and Its Applications, ICCSA 2020, held in Cagliari, Italy, in July 2020. Due to COVID-19 pandemic the conference was organized in an online event. Computational Science is the main pillar of most of the present research, industrial and commercial applications, and plays a unique role in exploiting ICT innovative technologies. The 466 full papers and 32 short papers presented were carefully reviewed and selected from 1450 submissions. Apart from the general track, ICCSA 2020 also include 52 workshops, in various areas of computational sciences, ranging from computational science technologies, to specific areas of computational sciences, such as software engineering, security, machine learning and artificial intelligence, blockchain technologies,

and of applications in many fields.

Holistic Approach to Quantum Cryptography in Cyber Security Concepts Books Publication

Advances in technology have provided numerous innovations that make people ' s daily lives easier and more convenient. However, as technology becomes more ubiquitous, corresponding risks also increase. The field of cryptography has become a solution to this ever-increasing problem. Applying strategic algorithms to cryptic issues can help save time and energy in solving the expanding problems within this field. Cryptography: Breakthroughs in Research and Practice examines novel designs and recent developments in cryptographic security control procedures to improve the efficiency of existing security mechanisms that can help in securing sensors, devices, networks, communication, and data. Highlighting a range of topics such as cyber security, threat detection, and encryption, this publication is an ideal reference source for academicians, graduate students, engineers, IT specialists, software engineers, security analysts, industry professionals, and researchers interested in expanding their knowledge of current trends and techniques within the cryptology field.

Computer Network Security IGI Global

This updated guide presents expert information on analyzing, designing, and implementing all aspects of computer network security. Based on the authors' earlier work, Computer System and Network Security, this new book addresses important concerns regarding network security. It contains new chapters on World Wide Web security issues, secure electronic commerce, incident response, as well as two new appendices on PGP and UNIX security fundamentals.

Springer Verlag

Privacy and security concerns are at the forefront of research and critical study in the prevalence of information technology. Pervasive Information Security and Privacy Developments: Trends and Advancements compiles research on topics such as technical, regulatory, organizational, managerial, cultural, ethical, and human aspects of information security and privacy. This reference offers methodologies, research frameworks, theory development and validation, case studies, simulations, technological architectures, infrastructure issues in design, and implementation of secure and privacy preserving initiatives.

Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection Springer Nature

This research study examines how information security visualization tools can be improved, by reviewing interactive and graphical techniques that could be used to address information overload. The use of information visualization tools in the defense of computer networks is growing. Providing tools that display information in a way that is useful is very important to network security. Novel but useful visualizations will enable the network security analysts to identify, analyze and if necessary remediate potentially malicious activity. This paper offers an overview of information visualization that discusses the information seeking mantra. The information seeking mantra shows what behaviors end users of information visualization tools expect. The topic of information overload is discussed as well as methodologies and frameworks developers can use to improve information visualization tools. Reference models and taxonomies are discussed that show how tool authors developed current tools. Developers can also find information on the interactive and graphical techniques. The graphical and interactive techniques are useful reference points for further study. Some of the themes from literature review include user-centered design, iterative development, and supporting basic user tasks. Limitations of this particular study and recommendations on future research provide the reader insight in ways that the field of information visualization can be expanded.

1979-1990 John Wiley & Sons

This book is a collection of selected papers presented at the First Congress on Intelligent Systems (CIS 2020), held in New Delhi, India during September 5 – 6, 2020. It includes novel and innovative work from experts, practitioners, scientists and decision-makers from academia and industry. It covers topics such as Internet of Things, information security, embedded systems, real-time systems, cloud computing, big data analysis, quantum computing, automation systems, bio-inspired intelligence, cognitive systems, cyber physical systems, data analytics, data/web mining, data science, intelligence for security, intelligent decision making systems, intelligent information processing, intelligent transportation, artificial intelligence for machine vision, imaging sensors technology, image segmentation, convolutional neural network, image/video classification, soft computing for machine vision, pattern recognition, human computer interaction, robotic devices and systems, autonomous vehicles, intelligent control systems, human motor control, game playing, evolutionary algorithms, swarm optimization, neural network, deep learning, supervised learning, unsupervised learning, fuzzy logic, rough sets, computational optimization, and neuro fuzzy systems.

Cryptocurrencies and Blockchain Technology Applications Springer Science & Business Media

The increased use of technology is necessary in order for industrial control systems to maintain and monitor industrial, infrastructural, or environmental processes. The need to secure and identify threats to the system is equally critical. Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection provides a full and detailed understanding of the vulnerabilities and security threats that exist within an industrial control system. This collection of research defines and analyzes the technical, procedural, and managerial responses to securing these systems.

Computational Science and Its Applications – ICCSA 2020 Elsevier

This book presents best selected research papers presented at the International Conference on Computer Networks, Big Data and IoT (ICCBI 2020), organized by Vaigai College Engineering, Madurai, Tamil Nadu, India, during 15 – 16 December 2020. The book covers original papers on computer networks, network protocols and wireless networks, data communication technologies and network security. The book is a valuable resource and reference for researchers, instructors, students, scientists, engineers, managers and industry practitioners in those important areas.

Computer and Network Security IGI Global

This book highlights the state-of-the-art research on data usage, security, and privacy in the scenarios of the Internet of Things (IoT), along with related applications using Machine Learning and Big Data technologies to design and make efficient Internet-compatible IoT systems. ICT and Data Sciences brings together IoT and Machine Learning and provides the careful integration of both, along with many examples and case studies. It illustrates the merging of two technologies while presenting basic to high-level concepts covering different fields and domains such as the Hospitality and Tourism industry, Smart Clothing, Cyber Crime, Programming, Communications, Business Intelligence, all in the context of the Internet of Things. The book is written for researchers and practitioners, working in Information Communication Technology and Computer Science.

Secure Computers and Networks Springer Nature

This book focuses on green computing-based network security techniques and addresses the challenges involved in practical implementation. It also explores the idea of energy-efficient computing for network and data security and covers the security threats involved in social networks, data centers, IoT, and biomedical applications. Green Computing in Network Security: Energy Efficient Solutions for Business and Home includes analysis of green-security

mechanisms and explores the role of green computing for secured modern internet applications. It discusses green computing-based distributed learning approaches for security and emphasizes the development of green computing-based security systems for IoT devices. Written with researchers, academic libraries, and professionals in mind so they can get up to speed on network security, the challenges, and implementation processes.

Proceedings of a Workshop on Deterring Cyberattacks Walter de Gruyter

As the advancement of technology continues, cyber security continues to play a significant role in today s world. With society becoming more dependent on the internet, new opportunities for virtual attacks can lead to the exposure of critical information. Machine and deep learning techniques to prevent this exposure of information are being applied to address mounting concerns in computer security. The Handbook of Research on Machine and Deep Learning Applications for Cyber Security is a pivotal reference source that provides vital research on the application of machine learning techniques for network security research. While highlighting topics such as web security, malware detection, and secure information sharing, this publication explores recent research findings in the area of electronic security as well as challenges and countermeasures in cyber security research. It is ideally designed for software engineers, IT specialists, cybersecurity analysts, industrial experts, academicians, researchers, and post-graduate students.

Computer and Network Security Essentials IGI Global

Network Security is a comprehensive resource written for anyone who plans or implements network security measures, including managers and practitioners. It offers a valuable dual perspective on security: how your network looks to hackers who want to get inside, and how you need to approach it on the inside to keep them at bay. You get all the hands-on technical advice you need to succeed, but also higher-level administrative guidance for developing an effective security policy. There may be no such thing as absolute security, but, as the author clearly demonstrates, there is a huge difference between the protection offered by routine reliance on third-party products and what you can achieve by actively making informed decisions. You ' ll learn to do just that with this book ' s assessments of the risks, rewards, and trade-offs related implementing security measures. Helps you see through a hacker's eyes so you can make your network more secure. Provides technical advice that can be applied in any environment, on any platform, including help with intrusion detection systems, firewalls, encryption, anti-virus software, and digital certificates. Emphasizes a wide range of administrative considerations, including security policies, user management, and control of services and devices. Covers techniques for enhancing the physical security of your systems and network. Explains how hackers use information-gathering to find and exploit security flaws. Examines the most effective ways to prevent hackers from gaining root access to a server. Addresses Denial of Service attacks, "malware," and spoofing. Includes appendices covering the TCP/IP protocol stack, well-known ports, and reliable sources for security warnings and updates.

Network Security Secure Computers and Networks

Cyber security is a key focus in the modern world as more private information is stored and saved online. In order to ensure vital information is protected from various cyber threats, it is essential to develop a thorough understanding of technologies that can address cyber security challenges. Artificial intelligence has been recognized as an important technology that can be employed successfully in the cyber security sector. Due to this, further study on the potential uses of artificial intelligence is required. Methods, Implementation, and Application of Cyber Security Intelligence and Analytics discusses critical artificial intelligence technologies that are utilized in cyber security and considers various cyber security issues and their optimal solutions supported by artificial intelligence. Covering a range of topics such as malware, smart grid, data breachers, and machine learning, this major reference work is ideal for security analysts, cyber security specialists, data analysts, security professionals, computer scientists, government officials, researchers, scholars, academicians, practitioners, instructors, and students.

The Network Security Center Springer Nature

This new book discusses the concepts while also highlighting the challenges in the field of quantum cryptography and also covering cryptographic techniques and cyber security techniques, in a single volume. It comprehensively covers important topics in the field of quantum cryptography with applications, including quantum key distribution, position-based quantum cryptography, quantum teleportation, quantum e-commerce, quantum cloning, cyber security techniques ' architectures and design, cyber security techniques management, software-defined networks, and cyber security techniques for 5G communication. The text also discusses the security of practical quantum key distribution systems, applications and algorithms developed for quantum cryptography, as well as cyber security through quantum computing and quantum cryptography. The text will be beneficial for graduate students, academic researchers, and professionals working in the fields of electrical engineering, electronics and communications engineering, computer science, and information technology.

Simulation in Computer Network Design and Modeling: Use and Analysis Springer

This book presents the proceedings of The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT-2020), held in Shanghai, China, on November 6, 2020. Due to the COVID-19 outbreak problem, SPIoT-2020 conference was held online by Tencent Meeting. It provides comprehensive coverage of the latest advances and trends in information technology, science and engineering, addressing a number of broad themes, including novel machine learning and big data analytics methods for IoT security, data mining and statistical modelling for the secure IoT and machine learning-based security detecting protocols, which inspire the development of IoT security and privacy technologies. The contributions cover a wide range of topics: analytics and machine learning applications to IoT security; data-based metrics and risk assessment approaches for IoT; data confidentiality and privacy in IoT; and authentication and access control for data usage in IoT. Outlining promising future research directions, the book is a valuable resource for students, researchers and professionals and provides a useful reference guide for newcomers to the IoT security and privacy field.